symmetry

MDPI

Article

Preferential Delegated Proof of Stake (PDPoS)—Modified DPoS with Two Layers towards Scalability and Higher TPS

Vishal Bachani [1] and Aniruddha Bhattacharjya [2,*]

[1] College of Natural and Applied Science, University of Houston-Victoria, Victoria, TX 77901, USA
[2] Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur 522502, Andhra Pradesh, India
* Correspondence: abthuee@kluniversity.in

Abstract: Security and a decentralized system are identical unique features of Blockchain. In recent times, blockchain-based cryptocurrency has become mainstream, but the growth and value of transactions and application services remain volatile. Among all these applications, finding a fast consensus in a large-scale blockchain network frequently requires extreme energy for huge computations and storing the complete blockchain for verification. These problems prevent further commercialization. Here, we present a solution to this problem. In this paper, we introduce a revised blockchain consensus algorithm, PDPoS, to address the scalability and transaction efficiency limitations. The symmetry in between Proof of Stake (PoS) and Delegated Proof of Stake (DPoS) is PoS. However, their ways of working are dissimilar. Here, we review the existing consensus algorithms, such as Proof of work (PoW), PoS and DPoS, as they are directly relating to our proposed work: PDPoS. We highligh Delegated Proof of Stake (DPoS)–based crypto-currencies, as they have much higher transactions per second (TPS) than PoW-based currencies. Then, we describe our proposed works and the working steps of the proposed PDPoS. Simulation results of the proposed PDPoS with two layers result in improved efficiency. We used TPS as the evolution criteria for showing that the proposed PDPoS is more efficient than DPoS. This makes the proposed work more relevant to the large-scale blockchain network as it is more efficient and requires less energy consumption.

Keywords: PoS; DPoS; PDPoS; Symmetry; Block Producer (BP); Super Block Producer (Super BP); Super Representatives (SRs); TPS; Casper the Friendly Finality Gadget (CFFG); Casper the Friendly Ghost (CTFG)

Citation: Bachani, V.; Bhattacharjya, A. Preferential Delegated Proof of Stake (PDPoS)—Modified DPoS with Two Layers towards Scalability and Higher TPS. *Symmetry* **2023**, *15*, 4. https://doi.org/10.3390/sym15010004

Academic Editor: Christos Volos

Received: 22 November 2022
Revised: 13 December 2022
Accepted: 13 December 2022
Published: 20 December 2022

1. Introduction

All transactions made in the blockchain are shared and available to all nodes. This feature increases the system's transparency in comparison with the centralized transactions with a third party. Additionally, all nodes in the blockchain are unidentified, resulting in other nodes confirming transactions with more safety. For the reason that blockchain is a decentralized system and excludes the necessity for a third-party intermediary, it is a prospective platform for exponential growth, similar to the Internet. Early blockchain application was largely restricted to cryptocurrency creation and transaction. Now blockchain-based cryptocurrency is becoming mainstream, but the growth and value of transactions and application services remain volatile [1]. In the last ten years, blockchain technology was also gradually applied to global supply chain management [2], Internet of Things (IoT) [3], health sectors [4], legal businesses [5], and most recently, the digital asset auction and management, Non-Fungible Tokens (NFTs) [6].

Among these applications, attaining a fast consensus in a large-scale blockchain network often necessitates too much energy for computing and storing the complete blockchain for verification, which becomes a technical problem in further commercialization in this modern era. In other words, the high transaction computing cost, or the so-called gas

fee, is limiting the growth and scalability of blockchain applications. To compete with centralized systems, blockchain technology must have a highly scalable structure that includes low transaction costs and increased bandwidth to accommodate more TPS. The most important contributing factor for addressing this issue is a proper consensus algorithm.

We know that dissimilar blockchain architectures are ever-present, so divergent classifications of consensus mechanisms are the foremost emphasis. In recent times, consensus mechanisms have had divergent features related to application spheres. Furthermore, they have had divergent functionalities related to real-time application spheres. We recognize that the RSA has a noteworthy part in secure communication [7–9]. The security characteristics of the IoT and Cyber-Physical System (CPS) are elaborated in depth along with their shortcomings in [10–13]. The in-depth evaluations of the SHRSA messaging scheme's cipher's method of operating and blockchain's consensus protocols' method of operating are deliberated in [14]. In addition, RSA can have a practical use in incorporation with the Peer to Peer (P2P) multilevel authenticated messaging schemes (secure hybrid RSA, SHRSA [15]). Blockchain is similar to a bundled technology, with its integral consensus schemes, end-to-end (E2E) secure protocols, and distributed data storage. These properties are seamlessly obligatory for CPS and IoT architectures [10–16]. There are numerous varieties of consensus protocols, including PoW and PoS as the two main categories [17].

This paper proposes a revised blockchain consensus algorithm PDPoS for addressing the scalability and transaction efficiency limitations. Section 2 focuses on related works. The cryptocurrencies using DPoS are discussed in Section 3. Section 4 describes the proposed PDPoS consensus algorithm, and Section 5 elaborates on the implementation and results. Finally, Section 6 concludes the paper and mentions future works.

2. Related Works

Using a particular consensus algorithm to reach an agreement on transactions among all participants in a blockchain network is a challenging task and a crucial procedure. In any blockchain network, new transaction records are uploaded constantly to the blockchain as all nodes in the network validate the new block. It is worth mentioning that blocks cannot be modified or removed once they have been validated. Blockchains are created to remain valid in a trustless and unstable network with confrontational users. Since the invention of blockchain, different approaches have been suggested and implemented as consensus algorithms. Here, we highlight the two most frequently used consensus algorithms and their advantages and disadvantages. Then, we discuss DPoS, as our work involves the modification of DPoS towards higher TPS and scalability.

A. POW

PoW was initially proposed as an idea to combat spam email (Hashcash) in 1997 and as a countermeasure of Denial of Service (DoS) Attack in 2002 [18]. In combating email spam, the idea is to create a hashcash stamp for attaching to an email to impose a microcost of sending emails in order to dissuade spammers. Hal Finney integrated this idea into the design of a cryptocurrency in 2005, but it fell short of the ideal by relying on trusted computing as a backend. PoW finally caught on with its further adaption into a decentralized computing platform or blockchain, as Bitcoin [19] and other cryptocurrencies such as Ethereum [20].

In a PoW-driven blockchain, each block contains the preceding block's hash value, transaction history, and nonce, along with current block's hash. For example, a miner or a computer attempting to solve the hash will look for a nonce that will cause the hash value to fulfill a preset criterion, such as finding the nonce that will make the hash value's first thirty bits zero.

Strong security and decentralization are the two advantages of the PoW algorithm. It provides the utility of mining and certifying blocks. On the other hand, it consumes a

great deal of energy, which is its biggest disadvantage. Furthermore, the speed and success rate of the hash function are greatly reliant on the processing capacity of the hardware that executes the hash [21]. Furthermore, while the hash function's complexity can be adjusted due to the difficulty of calculating the hash function, fixing this problem takes time. As a result, PoW is not appropriate for large, fast-growing business transactions. Therefore, the PoW consensus algorithm has the benefits of a decentralized structure, higher security, and better scalability. However, it has disadvantages in low throughput, long block creation time, energy inefficiency, reliance on unique hardware, high computational cost, and requiring much bandwidth.

To address the limitations of PoW, PoS was proposed and first implemented in cryptocurrency in 2012 as an alternative consensus algorithm with a much-reduced energy consumption [22].

B. POS

PoS is a blockchain consensus algorithm, in which a user can mine and certify block transactions based on their stake value instead of computational power. The algorithms need users to stake a particular amount of their tokens to give them a chance to be chosen for validating transaction blocks and receive a reward for doing so [23]. When a block of transactions is ready to be processed, the protocol selects validators based on each users' holdings to circumvent PoW's high computational costs. Once the validator verifies that the block's transactions are correct, they will add the block to the blockchain and be rewarded. If a validator adds a block with incorrect information, they will be penalized by losing some of their staked holdings.

Every user of the PoS platform must put a stake in the network by depositing a particular number of tokens. The stake is kept in a virtual safe and is used to guarantee the blocks. The validators' chances of being chosen are raised in proportion to the amount of money they are willing to risk. The bigger the stakes, the more likely a user will be chosen. There are variants of PoS protocol to choose validators, such as random selection, stake supply, and token age. However, although everybody staking tokens can be chosen as a validator, the chances are lower if one stakes only a tiny amount. Hence, the majority of PoS platform users join the so-called PoS Pool. The owner of the staking pool sets up the validator node, and a group of users pool their funds for a better chance of winning new blocks. The rewards are distributed among the pool's members, and the pool owner may charge a nominal fee [24]. One example is a validator selection protocol ("Casper") chosen by Ethereum; this is a random selection, and each block has to be validated in a limited timeframe by 128 randomly selected validators ("a committee") [25].

The limitations of PoS include centralization tendency and security concerns. For example, when a user node holds many stakes for a long time, its probability of being selected as a validator is nearly 100%. Hence, the protocol has the inherent limitation of making the PoS platform more centralized. PoS is also subjected to various security concerns, including Nothing at Stake and long-range attacks [26].

In addition, though PoS takes only 64 s to generate a block, which is comparatively much less than PoW, it still relies on computing power and wastes computing resources during each block generation process [27], which makes it less likely to be adopted in high frequency transaction scenarios, such as online retail payment.

C. DPoS

To further reduce the computing power consumption and processing time in generating new blocks, a Delegated PoS voting schema was proposed in [28]. In the DPoS, the reputation scores or other techniques are used for selecting the validators. Although it has the PoS name integrated with full form and it has symmetry with this part as per full form, factually it is relatively dissimilar to other PoS consensus protocols.

Blockchains that use DPoS rely on a reputation-based voting approaches to reach consensus. On a DPoS blockchain, holdings holders have the right to vote on which nodes should validate transactions. The size of the holdings he or she stakes decides the user's

voting power. Users who stake more holdings have more influence over who is elected to the nodes. These elected nodes are referred to as Delegates. All the nodes in the blockchain network have the right to vote as per the stakes and then can pick their own approved node in the classic DPoS process.

DPoS is more democratic by design than comparable systems, since it uses a decentralized voting procedure. Rather than eliminating the need for trust, DPoS has a procedure to check that those who are entrusted with signing blocks on behalf of the network are doing so correctly and impartially. Additionally, each signed block must verify that the block came from a trusted node. DPoS eliminates the need to confirm a transaction until a specific number of untrusted nodes have verified it. It also allows for more transactions to be included in a block than PoW or PoS. However, DPoS still has the disadvantages of less decentralization than PoW as well as security concerns [29]; however, it generally assists in providing faster processing-based transactions of around 3 s [28].

In DPoS, users vote for selecting a cluster of delegates that produce the blocks. The users make use of scores of reputations or other techniques for choosing the cluster of delegates. In DPoS, the delegates are the lone entities for proposing new blocks. In all the rounds, a leader is chosen from the cluster of representatives (delegates) who can produce the block in that specified network.

Choosing the forerunner (leader) is based on the corresponding system. The forerunners are rewarded for producing the new block, and if in the scenario they misbehave, they are de-listed from the cluster of validators.

All the representatives contend with one another for inclusion in the cluster of validators. In this scenario, each validator can offer dissimilar incentives for the voters intending to vote for it. For example, if a representative is chosen for proposing a block, it may dispense a definite fraction of the reward amount amongst the users who have chosen it. It is well understood that as validators' numbers are a few, the consensus will be fast at the end of the process.

3. DPoS-Based Crypto-Currencies

We found numerous mechanisms set up by dissimilar cryptocurrencies under the common category of DPoS [30,31]. The following are some examples of DPoS based crypto-currencies.

1. EOS is the foremost and the most extensively recognized DPoS crypto-currency [30,31]. It is also the smart-contract platform in its class. Better scalability and better transactions per second than Ethereum are the key features of EOS. In the Ethereum platform, the initial EOS currency is produced. Then, it is migrated to its very own Blockchain. A total of 21 validators are used by the DPoS consensus algorithm of EOS, acknowledged as BPs. These validators are chosen with votes from the holders of EOS token (currency). For a specific BP, the selection time (No. of times selected) for producing a block is proportionate to the total votes from the token owners. Every DPoS currency requires production of a preliminary supply in advance of the moment the network becomes functional. This supply is used for selecting 21 BPs (with voting) in addition to the incentive the BPs have for producing blocks, resulting in a secure network. Currently, an EOS block is produced in 0.5 s. Blocks in EOS are created in rounds, and every round comprises the mentioned number of blocks. At the commencement of each round, the mentioned number of BPs (21) are chosen. Afterward, each of them has an opportunity to produce a block in a pseudo-random manner inside that specific round. As soon as a BP creates a block, other BPs are required to validate the block, and afterward consensus is attained. A block is established in the case that most of the BPs come to a consensus concerning the legitimacy of the block. Whenever this occurs, the block along with the allied transactions are valid or confirmed, so there are no possibilities for forks to take place.

2. Tron is also a widespread cryptocurrency depending on DPoS [30,31]. Its consensus algorithm uses 27 validators, recognized as SRs. The SRs are chosen every six hours by the votes from TRX holders, who must freeze a definite amount of TRX for voting for an SR. The deposit sum may be frozen back exactly three days after the casting of the votes. A block in Tron is produced every 3 s for the conforming SR, obtaining an incentive of 32 TRX. One more significant property of the Tron is that no inflation (in-built) mechanism is present in the protocol; this denotes that the entire supply will endure through its lifetime.
3. Tezos also makes use of a variation of DPoS consensus [30,31]. It is similar to EOS and Tron. With a block incentive of 16 XTZ (currency of Tezos) and block production time of 60 s, any predefined number of Bakers (as defined in Tezos) is not necessary for Tezos. Here, Bakers are just stakeholders. This way, Tezos differs from other DPoS-based currencies. As an alternative, the consensus mechanism makes use of a dynamic range of stakeholders, where someone holding a considerable amount of XTZ might be a stakeholder. This stops common users from participating in the consensus mechanism. For resolving this problem, Tezos make available a mechanism in which all can give XTZ to anyone. As a result, it can gather the obligatory XTZ numbers for becoming a baker. In response to this, the baker would back a definite proportionate amount of their received block incentive to the delegated party.
4. Lisk is a distinctive DPoS-based platform empowering the expansion of DApps by the use of JavaScript [30,31]. One more unique property of Lisk is its capability to host and then to function with several blockchains, known as sidechains, together with a central blockchain, known as a mainchain. All sidechains can be set up and upheld by a specific application facilitator, whose prerequisite is to be synchronous with the mainchain based on Lisk's protocol. As a result, dissimilar applications can leverage dissimilar sidechains concurrently, thus not troubling the mainchain. Here, only 101 delegates can be used to yield a block. These delegates are chosen by votes from Lisk currency (denoted with LSK) owners. Here, each holder has a specified number of votes. In addition, the weight of a vote is proportionate to the summation of LSK owned by the corresponding owner. The event of choosing the delegates occurs before the round, where each round comprises a specified number of block generation cycles. Thus, in a round, each delegate is arbitrarily chosen for creating a block. The block production time is 10 s. The block reward is 5 LSK.
5. Ark is also a distinctive DPoS-based blockchain platform [30,31]. It makes use of 51 delegates for producing 51 blocks in each round. The block creation time of Ark is 8 s, and each round goes on for 408 s. Each delegate gets 2 ARK for producing a block. The delegates in Ark are chosen by the votes of the owner of the Ark currency; here, the weight of each is proportionate to the voter's ARK amount.

The reported TPS for Bitcoin and Ether (Currency of Ethereum platform) are 7 and 15–25, correspondingly [30,31]. The DPoS currency EOS has an informed and estimated TPS of 50 and 4000, correspondingly, and Tron has TPS of 2000 [30,31]. Undoubtedly, DPoS currencies have much better enactment than PoW currencies in terms of TPS.

4. Proposed PDPoS

For further reduction of the transaction cost and improving the transaction efficiency per second for DPoS, we propose a revised DPoS schema, the PDPoS. The PDPoS is a tweak to the existing DPoS consensus, and it permits blockchain to have a Layer 2 network on top of the present network, as shown in Figure 1. We also introduce the concept of Super BP.

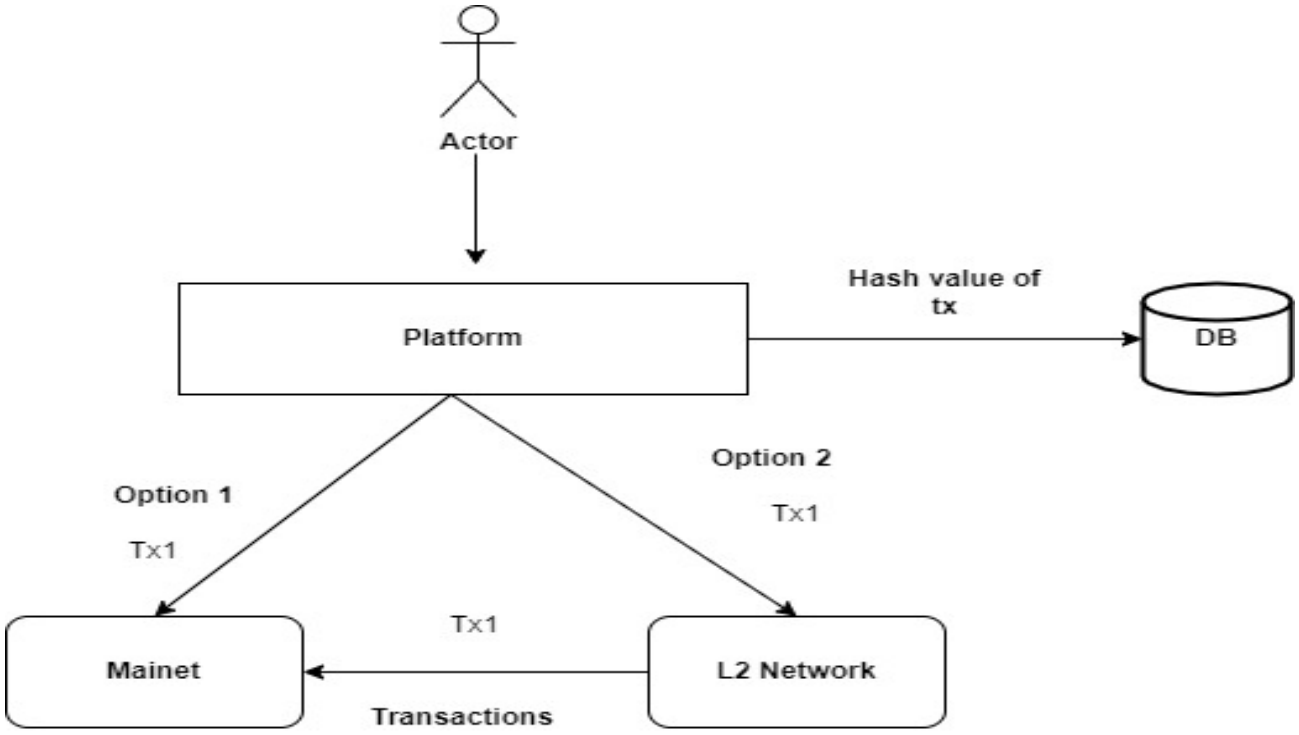

Figure 1. A Revised L2 Solution on DpoS.

We assume that a user uses a blockchain-based platform and finishes a transaction. The user will send it to L2 or the mainnet for processing. The L2 transaction would be less expensive as compared to the mainnet transaction. The transaction that goes straight to the mainnet is called "Preferential Delegated of Stake" [32].

The user will be paying more as it will reach inevitability faster than the L2. The mainnet would have DPoS, but block creators would have to stake more tokens for validating the transaction, and the voting and the validating incentives must be higher than on the L2 network.

The L2 network would also be responsible for DPoS consensus, but the transaction would not be confirmed, and the user would be paying more to send the transaction straight to L1. Every transaction on L2 would ultimately become part of the mainnet. This would occur after 24 h or on every occasion the throughput to the mainnet is tremendously low (limits to be determined).

At the same time, the block producers of L2 cannot take part in mainnet, and vice versa. Since L2 would have lower gas prices, the reward for validating would be less. On the mainnet, L2 TPS is anticipated to be around 60,000, with a transaction rate of approximately 20,000 [32].

The number of block makers would vary between the L2 and mainnet transactions; the mainnet would have 24 block makers, and the L2 would have 12.

This consensus protocol would upsurge the network's transaction speed by decongesting the mainnet. It also allows the users to receive benefit from the blockchain with a lower price. This agreement would permit customers to pay as per the urgency and use case. The customers would trace their transactions and obtain an update when they transfer from L2 to mainnet. If the user is in a hurry to have the transaction authenticated, they will have to pay an extra cost, but the transaction will travel straight to the network and receive an prompt confirmation. To store the hash, the platform will use an external database to be used in the scenario of a missed or failed transaction from L2 to mainnet [32].

To be a BP on the mainnet, one must have a specific amount of processing power and hold a stake for a definite period. Following the completion of the time, the BPs would enter the election pool, where community members would vote on the BPs every hour.

There would be 24 Block Producers, with the top four being identified as Super BPs. To achieve finality, transactions must be validated by a minimum of 20 BPs, and at least three of the four super BPs must sign and validate the transaction, or else the transaction will not be validated. The network's efficiency and security will both improve because of this. After every hour, elections help to decide the fate of the next BP over the next one-hour period.

The identical mechanism can be applied to the L2, except that the number of BPs would be reduced to 10, and the concept of a Super BP would be eliminated. Every hour, an election would be held. The BP has to stake fewer tokens, and the time will be shorter. The voting reward will be the same as the mainnet vote reward.

In our PDPoS as shown in Figure 2, every user in the network will receive a reward. Both Super BPs and BPs will be compensated based on the number of blocks they validate each hour. The voting prizes will also be given to the voters. This network could be utilized for high-frequency instantaneous transactions as well as deferred payment transactions.

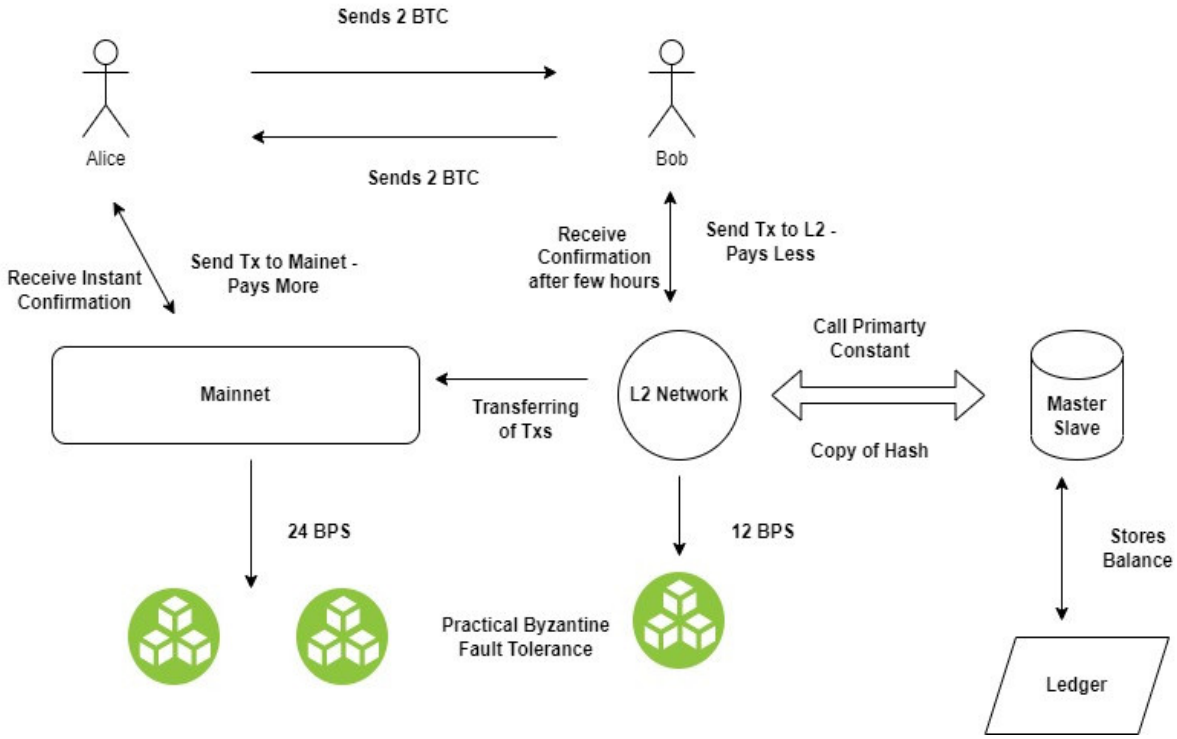

Figure 2. An Illustration of a Preferential DPoS Transaction.

To save the network from malicious transactions and double spending, the platform is equipped with Practical Byzantine Fault Tolerance (pBFT) and incorporates Master–Slave Architecture, where a copy of each transaction would be stored in case of the transaction being rejected from L2 to mainnet.

The step-by-step processes of the PDPoS are described here-

(1) SELECTION OF CONSENSUS NODES

- This particular blockchain is divided into two layers, i.e., Layer 1 and Layer 2.
- The final settlement happens on Layer 1 (transaction will go into finality).
- Each Layer 1 and Layer 2 work on delegate proof of mechanism.
- Layer 1 has 24 block producers, with each elected from the community and by the community.
- Layer 2 has 12 block producers, with each block producer contributing to the community.

- Each layer is secure for avoiding malicious transactions and double-spending.

(2) BLOCK PRODUCER NOMINATION PROCEDURE

- The block producers for Layer 1 are nominated using by-elections, by the community members.
- The block producers for Layer 1 contribute and are part of the chain for at least 2 weeks in order to be nominated for block producer and also after being a block producer on the layer for 2 weeks.
- The block producer nomination procedure for layers also requires the producers to stake a particular number of coins.
- The block producers for Layer 2 are nominated based on the contribution of the community.
- The Layer 1 block producer is compensated for the number of transactions they approve.

(3) JOURNEY OF TRANSACTION

- The users have the option to choose where they intend to send the transaction: either Layer 1 or Layer 2.
- Users wanting to send directly to Layer 1 would have to pay a higher fee and can achieve transaction finality within a few seconds.
- Users wanting to send via Layer 2 have minimal fees, but their transaction finality will come in (T + 1) time.
- The transactions at Layer 2 are bundled up and sent to Layer 1 every 12 h.
- This bundled transaction is optimized so that lesser fees are required for them to reach finality.

Pseudocode ALGORITHM

LET Blockchain Network into **Layer 1(L1) and Layer 2(L2)**
If (Block Producer == Layer 1) {
LET More Staking Requirements
LET More Staking Time Period
LET Community Members VOTE BP
LET Them serve layer 2 for weeks
LET Number of BP == 24
}
If (Block Producer == Layer 2) {
LET LESS Staking Requirements
MORE Contribution to the ov
LET Community Members choose BP
LET Number of BP == 12
}
IF (USERS == VOTE){
(IF VOTE == Layer 1 BLOCK PRODUCER 1)
LET MORE STAKING
LET Number of Votes == 4 Separate Block Producers
(IF VOTE == Layer 2 BLOCK PRODUCER 1)
LET NO Staking Requirement
LET Number of Votes == 2 Separate Block Producers

}

L1 && L2 are two layers of **Blockchain Network (BN)**
INITIATE Transaction (Tx) by Customers.
LET Customer choose from **L1 or L2.**

IF(CHOICE == Layer 1) {
INSERT TX Directly in Layer 1
Gas Fees == More From Customers.
}

IF(CHOICE == Layer 2) {
INSERT TX in Layer 2
BATCH all the Transactions (TXX)
INSERT TXX in Layer 1 After a certain allocated time
Gas Fees == LESS From Customers.
}

Reward Distribution

IF (BP == Layer 1)
{
LET Reward == Number of Transaction Approved
Reward == 0.5 Gas Fees of Each Block
IF (BP == Layer2)
{
LET Reward == Number of Transaction Approved
LET Reward == More Coins staked
Helps them to Layer 1 BP
}

5. Implementation of the PDPoS Algorithm

Here, we describe the implementation in three parts.

A. Transaction Per Second for Normal Blockchain

TPS = Transactions per Second
Number of Block Producers = (BPs)
Number of Transactions = (Tx)
Number of Blocks Produced in One Second = (Ti)

$$TPS = \{BPs, Ti, Tx\}\text{-------}\ \alpha$$

Keeping Ti Constant

$$TPS \propto BP \;\&\&\; Tx.$$

$$TPS = K\ BP \;\&\&\; TX\text{-------}\beta$$

where K is the proportionality constant

$$BP = \sum (BPi, BPii, \ldots . BPn)$$

B. Transaction Per Second for Blockchain with PDPOS

Dividing blockchain into two layers: Layer 1 (li) and Layer 2 (Lii)
For each layer, the BP would be

$$BP(li) = \sum (BP1, BP2 \ldots BPN)$$

$$BP(lii) = \sum (BP12, BP22 \ldots . BP(n/2)$$

Dividing Transaction (Tx) into two parts:

Tx—Lii -- > Li (Tx coming in main layer via *Layer 2 Lii)*
Tx---> Li (Tx coming directly to main layer Li)
Suppose the number of Tx going directly to main layer (Li) after Lii was introduced,

$$NewTx = (tx/2)$$

Since TPS == K BP
Now TPS To Main Layer Li

$$TPS = K\{KBP(li), KBP(Lii)\}$$

TPS to Second Layer Lii

$$TPS = KBP(Lii)$$

C. Rate of Increase of Transaction Per Second for Blockchain with PDPOS

$$Cumulative\ TPS = \{KBP(Li), KBP(lii)\} + P(Lii)$$

$$Final\ TPS = \{KBP(Li), KBP(Lii)\} + P(Lii) + tx/2$$

The increase in block producer numbers at multiple layers and the decrease in direct transactions to the main layer result in the increase of TPS.

We use EOS Blockchain to carry out the following simulations.

Here, we show two simulation results: in Figure 3, the TPS with one layer, and in Figure 4, the TPS with 2 layers; in each case, there are 24 blocks.

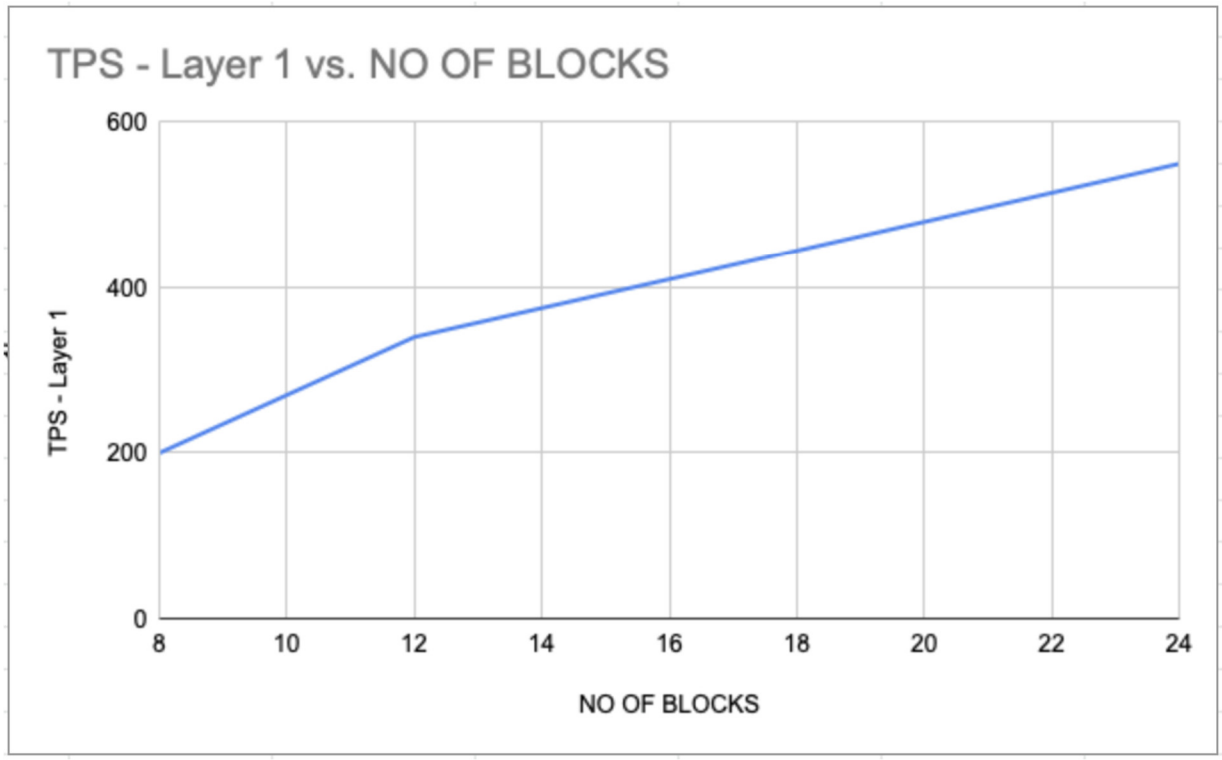

Figure 3. TPS With Layer—01.

In Figure 3, we show the corresponding TPS with layer 1 and 24 blocks. In Figure 4, we show the corresponding TPS with 1 layer (blue color) and with two layers (red color).

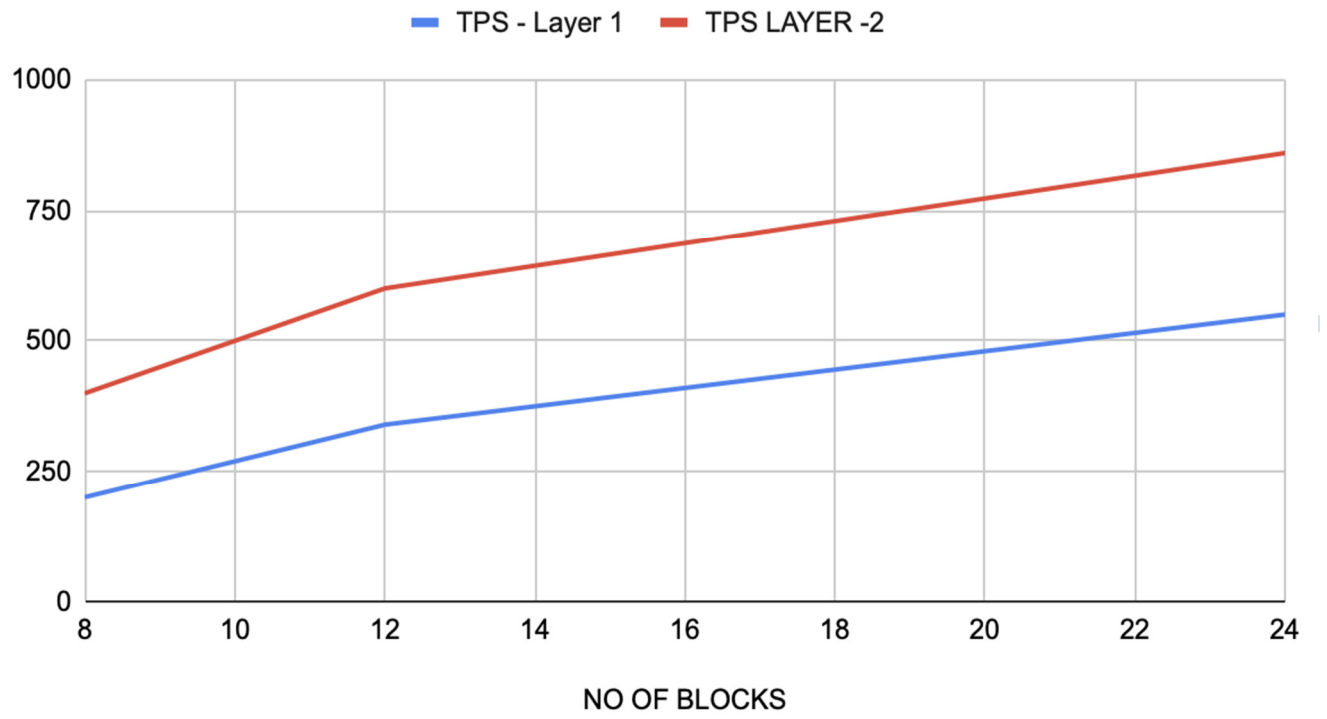

Figure 4. TPS With Layer—01 and 02.

Here, we can see that with 24 Blocks, for Layer 1, the TPS is just 500, but with Layer 2, it is near 900 (above 750 with 20 Blocks). Thus, it is clear from the Figure 4 that with Layer 2 the TPS increased significantly; with 24 Blocks, we are gaining nearly 400 TPS. Thus, for each Block, we gain a TPS of approximately 16.67 (400/24). In other words, average TPS gain of PDPoS in comparison with DPoS is 16.67.

Our proposed PDPoS is more efficient than the DPoS. For large-scale financial sectors, higher TPS is desirable. Higher TPS also means less consumption of energy.

Thus, higher energy efficiency comes with the reduced computing time needed due to increased TPS. Recently, Blockchain technology has been used increasingly [33–36] in areas like academia, industry, and government sectors. In the present era, there is a plethora of Blockchain architectures in various domains. This kind of consensus PDPoS with improved TPS is more suitable for large-scale financial transaction systems in the modern era.

6. Conclusions and Future Works

The aim of this blockchain is to replace the current financial system. This fast blockchain would enable easy and seamless transactions and transfers. This would enable people from across the globe to transfer their fiat money using stable coins. The fast TPS and lower gas fees would enable greater adoption of blockchain around the world.

PoW has the first-mover benefit because Bitcoin and Ethereum are the forerunners in their corresponding domains. It is a well-known fact that Bitcoin is the most-used cryptocurrency. The cryptocurrency is Ether for this platform. Many crypto-currencies, inspired by increased use, may utilize PoW as their conforming consensus protocol.

Another thing in favor of PoW is its fundamental security. The miners' number is much higher in Bitcoin in comparison with the validators' number in PoS and DPoS. This indicates that there is better decentralization in Bitcoin in comparison with PoS or DPoS. EOS has only 21 validators, while Tron has 27 validators. The possibility of collusion amongst these validators is much higher than PoW currency. Due to this, in the blockchain community, many are uncertain about the security of any PoS/DPoS currency. For mining centralization, many have the opinion that PoW also has a chance to be inclined to

centralization. Thus, collusion attacks on PoW can be a reality. With the supremacy of PoW over other consensus protocols, it can be said that there will be experiments with a changing balance in the near future. The CFFG and CTFG have been well studied by academics and industrialists, ensuring their robust security. Specifically, validators' numbers will be greater than any number leveraged in the present era's PoS/DPoS. However, it is yet to be determined how this will achieve once employed in everyday use.

This PDPoS will be very much suitable for application domains that require high-frequency transactions, such as online payment, due to its efficiency. Here, we used TPS as the evolution criteria.

In the near future, we plan to use multiple evaluation criteria, including Throughput, Block time/Latency, Profitability of Mining, Power consumption, Decentralization levels, Security and Mining Reward, and weighted scores for each criterion for testing and comparison.

Author Contributions: Conceptualization, V.B. and A.B.; methodology, V.B.; software, V.B.; validation, V.B. and A.B.; formal analysis, V.B.; investigation, V.B.; resources, V.B. and A.B.; data curation, V.B. and A.B.; writing—original draft preparation, V.B. and A.B.; writing—review and editing, A.B.; visualization, A.B.; supervision, A.B.; project administration, V.B. and A.B.; funding acquisition, A.B. All authors have read and agreed to the published version of the manuscript.

Funding: This work is partially supported by Research Incentives of the Koneru Lakshmaiah Education Foundation.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: This research is partially supported by Research Incentives of the Koneru Lakshmaiah Education Foundation.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Hajric, V.; Greifeld, K. Bitcoin went mainstream in 2021. It's just as volatile as ever. *Bloomberg Businessweek*, 21 December 2021.
2. Saberi, S.; Kouhizadeh, M.; Sarkis, J.; Shen, L. Blockchain technology and its relationships to sustainable supply chain management. *Int. J. Prod. Res.* **2019**, *57*, 2117–2135. https://doi.org/10.1080/00207543.2018.1533261.
3. Wang, Q.; Zhu, X.; Ni, Y.; Gu, L.; Zhu, H. Blockchain for the IoT and industrial IoT: A review. *Internet Things* **2020**, *10*, 100081. https://doi.org/10.1016/j.iot.2019.100081.
4. Abdellatif, A.A.; Samara, L.; Mohamed, A.; Erbad, A.; Chiasserini, C.F.; Guizani, M.; O'Connor, M.D.; Laughton, J. Medgechain: Leveraging edge computing and blockchain for efficient medical data exchange. *IEEE Internet Things J.* **2021**, *8*, 15762–15775.
5. Alston, E. Blockchain and the Law–Legality, Law-like Characteristics, and Legal Applications. In *The Economics of Blockchain and Cryptocurrency*; Edward Elgar Publishing: Cheltenham, UK, 2021.
6. Wang, Q.; Li, R.; Wang, Q.; Chen, S. Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges. 2021. Available online: http://arxiv.org/abs/2105.07447 (accessed on 30 October 2022).
7. Bhattacharjya, A.; Zhong, X.; Wang, J. Strong, efficient and reliable personal messaging peer to peer architecture based on Hybrid RSA. In Proceedings of the International Conference on Internet of Things and Cloud Computing (ICC 2016), Cambridge, UK, 22–23 March 2016; Association for Computing Machinery: New York, NY, USA, 2016; ISBN 978-1-4503-4063-2/16/03.
8. Bhattacharjya, A.; Zhong, X.; Wang, J. An end-to-end user two-way authenticated double encrypted messaging scheme based on hybrid RSA for the future internet architectures. *Int. J. Inf. Comput. Secur.* **2018**, *10*, 63–79. https://doi.org/10.1504/ijics.2018.089593.
9. Bhattacharjya, A.; Zhong, X.; Wang, J.; Li, X. Hybrid RSA-based highly efficient, reliable and strong personal full mesh networked messaging scheme. *Int. J. Inf. Comput. Secur.* **2018**, *10*, 418–436. https://doi.org/10.1504/ijics.2018.095341.
10. Bhattacharjya, A.; Zhong, X.; Wang, J.; Xing, L. Security Challenges and Concerns of Internet of Things (IoT). In *Cyber-Physical Systems: Architecture, Security and Application*; Guo, S., Zeng, D., Eds.; Springer: Cham, Switzerland, 2019; pp. 153–185.
11. Bhattacharjya, A.; Zhong, X.; Wang, J.; Xing, L. Secure IoT Structural design for Smart Cities. In *Smart Cities Cybersecurity and Privacy*; Elsevier: Amsterdam, The Netherlands, 2019; pp. 187–201.
12. Li, X.; Wang, J.; Zhong, X.; Bhattacharjya, A. On Mapping of Address and Port using Translation (MAP-T). *Int. J. Inf. Comput. Secur.* **2018**, *10*, 1. https://doi.org/10.1504/IJICS.2018.10008372.

13. Bhattacharjya, A.; Zhong, X.; Li, X. A Lightweight and Efficient Secure Hybrid RSA (SHRSA) Messaging Scheme With Four-Layered Authentication Stack. *IEEE Access* **2019**, *7*, 30487–30506. https://doi.org/10.1109/access.2019.2900300.
14. Bhattacharjya, A.; Zhong, X.; Wang, J.; Li, X. Present Scenarios of IoT Projects with Security Aspects Focused. In *Digital Twin Technologies and Smart Cities; Internet of Things: Digital Twin (Technology, Communications and, Computing)*; Farsi, M., Daneshkhah, A., Hosseinian-Far, A., Jahankhani, H., Eds.; Springer: Cham, Switzerland, 2020; pp. 95–122. https://doi.org/10.1007/978-3-030-18732-3_7.
15. Bhattacharjya, A.; Zhong, X.; Wang, J.; Li, X. CoAP—Application Layer Connection-Less Lightweight Protocol for the Internet of Things (IoT) and CoAP-IPSEC Security with DTLS Supporting CoAP. In *Digital Twin Technologies and Smart Cities; Internet of Things (Technology, Communications and Computing)*; Farsi, M., Daneshkhah, A., Hosseinian-Far, A., Jahankhani, H., Eds.; Springer: Cham, Switzerland, 2020; pp. 151–175. https://doi.org/10.1007/978-3-030-18732-3_9.
16. Bhattacharjya, A.; Zhong, X.; Wang, J.; Li, X. A Secure Hybrid RSA (SHRSA)-based Lightweight and Efficient Personal Messaging Communication Protocol. In *Digital Twin Technologies and Smart Cities; Internet of Things (Technology, Communications and Computing)*; Farsi, M., Daneshkhah, A., Hosseinian-Far, A., Jahankhani, H., Eds.; Springer: Cham, Switzerland, 2020; pp. 191–212. https://doi.org/10.1007/978-3-030-18732-3_11.
17. Bouraga, S. A taxonomy of blockchain consensus protocols: A survey and classification framework. *Expert Syst. Appl.* **2020**, *168*, 114384. https://doi.org/10.1016/j.eswa.2020.114384.
18. Back, A. Hashcash-A Denial of Service Counter-Measure; p. 9. 2002. Available online: http://hashcash.org/papers/hashcash.pdf (accessed on 30 December 2021).
19. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: www.bitcoin.org (accessed on 30 December 2021).
20. Burterin, V. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. 2013. Available online: https://ethereum.org/en/whitepaper/ (accessed on 30 October 2022).
21. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the 2017 IEEE International Congress on Big Data (Big Data congress), Honolulu, HI, USA, 25–30 June 2017; pp. 557–564.
22. King, S.; Nadal, S. PPcoin: Peer-to-peer crypto-currency with proof-of-stake. *Self-Publ. Pap.* **2012**, *19*, 2.
23. Larimer, D. Transactions as Proof-of-Stake, Ethereum Development Documentation. 2013. Available online: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/ (accessed on 30 December 2021)
24. Karakostas, D.; Kiayias, A.; Larangeira, M. Conclave: A collective stake pool protocol. In *European Symposium on Research in Computer Security*; Springer: Cham, Switzerland, 2021; pp. 370–389.
25. Buterin, V.; Griffith, V. Casper the friendly finality gadget. *arXiv* **2017**, arXiv1710.09437.
26. Li, W.; Andreina, S.; Bohli, J.-M.; Karame, G. Securing Proof-of-Stake Blockchain Protocols. In *Data privacy Management, Cryptocurrencies and Blockchain Technology*; Springer: Manhattan, NY, USA, 2017; pp. 297–315. https://doi.org/10.1007/978-3-319-67816-0_17.
27. Vasin, P. Blackcoin's Proof-of-Stake Protocol v2. 2014. Available online: http://cryptochainuni.com/wp-content/uploads/blackcoin-pos-protocol-v2-whitepaper.pdf (accessed on 30 October 2022).
28. Bitshares. Delegated Proof of Stake (DPOS). 2016. Available online: https://how.bitshares.works/en/master/technology/dpos.html (accessed on 30 October 2022).
29. Nguyen, C.T.; Hoang, D.T.; Nguyen, D.N.; Niyato, D.; Nguyen, H.T.; Dutkiewicz, E. Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities. *IEEE Access* **2019**, *7*, 85727–85745. https://doi.org/10.1109/access.2019.2925010.
30. Wang, W.; Hoang, D.T.; Hu, P.; Xiong, Z.; Niyato, D.; Wang, P.; Wen, Y.; Kim, D.I. A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. *IEEE Access* **2019**, *7*, 22328–22370. https://doi.org/10.1109/access.2019.2896108.
31. Xiao, Y.; Zhang, N.; Lou, W.; Hou, Y.T. A Survey of Distributed Consensus Protocols for Blockchain Networks. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1432–1465. https://doi.org/10.1109/comst.2020.2969706.
32. Bachani, V.; Wan, Y.; Bhattacharjya, A. *Preferential DPoS: A Scalable Blockchain Schema for High-Frequency Transaction*; AMCIS TREOs: Minneapolis, MN, USA, 2022.
33. Bamakan, S.M.H.; Motavali, A.; Bondarti, A.B. A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Syst. Appl.* **2020**, *154*, 113385. https://doi.org/10.1016/j.eswa.2020.113385.
34. Bhattacharjya, A. A holistic study on use of Blockchain technology in CPS and IoT architectures with focus on maintaining CIA triad of data communication. *Int. J. Appl. Math. Comput. Sci.* **2022**, *32*, 403–413.
35. Bhattacharjya, A.; Kozdrój, K.; Bazydło, G.; Wisniewski, R. Trusted and Secure Blockchain-Based Architecture for Internet-of-Medical-Things. *Electronics* **2022**, *11*, 2560. https://doi.org/10.3390/electronics11162560.
36. Bhattacharjya, A.; Wisniewski, R.; Nidumolu, V. A holistic research on major Blockchain's Consensus Protocols' working mechanisms with security aspects of CPS. *Electronics* **2022**, *11*, 2760.